National Phase of PCT/EP99/06312 in U.S.A.
Title: Device for supplying output data in reaction to input data and method for checking authenticity and method for encrypted data transmission
Applicants: OELMAIER; BRAND; HEUER; GERHAEUSER; PROSCH; KORTE; PLANKENBÜHLER

Translation of PCT Application PCT/EP99/06312
as originally filed

National Phase of PCT/EP99/06312 in U.S.A.

Title: Device for supplying output data in reaction to input data and method for checking authenticity and method for encrypted data transmission

Applicants: OELMAIER; BRAND; HEUER; GERHAEUSER; PROSCH; KORTE; PLANKENBÜHLER

Translation of Amendments under Art. 34 PCT
as attached to the IPER

It goes without saying that there are also mechanical protection mechanisms against such attacks, these protection mechanisms preventing e.g. access from outside to the card when the card has been inserted into a read unit. However, as has been described in the technical publication "Tamper Resistance A Cautionary Note; Proceedings – The Second USENIX Workshop on Electronic Commerce" by Markus Kuhn and Ross Anderson, there are a great number of counterfeiting methods which underline the unabating demand for better protection mechanisms for circuits and especially for integrated circuits on a chip card also in the future. Although conventional data encryption methods, which are based e.g. on the DES algorithm (DES Data Encryption Standard) or which comprise check sum algorithms, provide a high degree of safety when the encryption key, which together with the cryptoalgorithm permits decryption, is kept secret, it is, in principle, also here possible to imitate such an algorithm, which is integrated in a chip card in the form of an integrated circuit in terms of hardware, on the basis of the hardware implementation, i.e. to simulate the functionality of this algorithm e.g. by means of a computer.

~~It is the object of the present invention to provide a concept for improved protection of elec~~tronic circuits and to provide thus a counterfeit-proof check of the authenticity of such electronic circuits and a counterfeit-proof authorization of an owner of such electronic circuits.

This object is achieved by a device according to claim 1 and by a method according to claim 17 or 18.

The present invention is based on the finding that it is comparatively simple to imitate the functionality of a chip, but that it is much more difficult to imitate its time or power behaviour. A device for supplying output data in reaction to input data so as to determine the authenticity of the device in dependence upon said output data comprises therefore, on the one hand, an electronic circuit for executing an algorithm that generates the output data on the basis of the input data, and, on the other hand, a unit for detecting operational data which are influenced by an operation of the electronic circuit, the data detection unit being coupled to the electronic circuit in such a way that the operational data of the electronic circuit ~~are used by the algorithm for generating the output data~~.

→ page 3a

EP 0 313 967 refers to a method for checking the authenticity of a data carrier with an integrated circuit. A card comprises a memory consisting of an area which is accessible from outside and of an area which is not accessible from outside for storing confidential information, e.g. a key, etc.. The card additionally comprises a measuring circuit for determining the individual characteristic data of the card, such as the programming times of E^2PROM cells of the memory. The measuring circuit is connected to the memory and may be provided with additional processing means for processing the measured data. The card additionally comprises an encryption means which, making use of a key which is also stored in the memory, encrypts the individual characteristic data of the storage cell as well as a random number transmitted from a main station, so as to generate an encrypted output value which is decrypted at a main station with a corresponding key so that the random number on the one hand and the individual characteristic data of the memory on the other will be obtained again. The individual characteristic data of the memory are always the same, independently of the random number fed into the card. The re-decrypted random number is compared with the random number transmitted from the central station to the card. The ascertained individual characteristic data of the storage cell are checked with characteristic data stored at the central station. If both the random numbers and the characteristic data correspond, it is assumed that the card checked is authentic. If the random numbers correspond, whereas the individual characteristic data are different, it can be assumed that the card in question is a counterfeited card whose functionality corresponds to that of the authentic card, but whose characteristic data are different.

→ page 3b

~~It goes without saying that there are also mechanical protection mechanisms against such~~ attacks, these protection mechanisms preventing e.g. access from outside to the card when the card has been inserted into a read unit. However, as has been described in the technical publication "Tamper Resistance A Cautionary Note; Proceedings - The Second USENIX Workshop on Electronic Commerce" by Markus Kuhn and Ross Anderson, there are a great number of counterfeiting methods which underline the unabating demand for better protection mechanisms for circuits and especially for integrated circuits on a chip card also in the future. Although conventional data encryption methods, which are based e.g. on the DES algorithm (DES Data Encryption Standard) or which comprise check sum algorithms, provide a high degree of safety when the encryption key, which together with the cryptoalgorithm permits decryption, is kept secret, it is, in principle, also here possible to imitate such an algorithm, which is integrated in a chip card in the form of an integrated circuit in terms of hardware, on the basis of the hardware implementation, i.e. to simulate the ~~functionality of this algorithm e.g. by means of a computer~~.

It is the object of the present invention to provide a concept for improved protection of electronic circuits and to provide thus a counterfeit-proof check of the authenticity of such electronic circuits and a counterfeit-proof authorization of an owner of such electronic circuits.

This object is achieved by a device according to claim 1 and by a method according to claim 17 or 18.

The present invention is based on the finding that it is comparatively simple to imitate the functionality of a chip, but that it is much more difficult to imitate its time or power behaviour. A device for supplying output data in reaction to input data so as to determine the authenticity of the device in dependence upon said output data comprises therefore, on the one hand, an electronic circuit for executing an algorithm that generates the output data on the basis of the input data, and, on the other hand, a unit for detecting operational data which are influenced by an operation of the electronic circuit, the data detection unit being coupled to the electronic circuit in such a way that the operational data of the electronic circuit are used by the algorithm for generating the output data.

→ page 4

CLAIMS

1. A device (10) for supplying output data (12) in reaction to input data (14), comprising:

an electronic circuit (16) for executing an algorithm so as to generate the output data (12) on the basis of the input data (14); and

a unit (18) for detecting operational data of the electronic circuit (16) which are influenced by an operation of said electronic circuit (16) when said electronic circuit (16) executes the algorithm, the operational data depending on the input data,

said operational data detection unit (18) being coupled to the electronic circuit (16) in such a way that the detected operational data of the electronic circuit are used by the algorithm, which is executed by said electronic circuit (16), for generating the output data (12), whereby the authenticity of the device (10) is determined on the basis of the output data.

2. A device (10) according to claim 1, wherein the operational data are selected from the group comprising time data and power data.

3. A device (10) according to claim 1 or 2, wherein the electronic circuit (16) and the detection unit (18) are integrated as a unit.

4. A device (10) according to one of the preceding claims, which is contained in a smart card or in a PC card.

5. A device (10) according to one of the preceding claims, wherein the electronic circuit (16) is arranged so as to execute an cryptoalgorithm.

6. A device (10) according to one of the claims 1 to 4, wherein the electronic circuit (16) is arranged so as to execute a check sum algorithm.

7. A device (10) according to claim 5, wherein the cryptoalgorithm is a multi-step algorithm, the operational data of one algorithm step being used as input data for the subsequent algorithm step.

8. A device (10) according to one of the claims 1 to 6, wherein the electronic circuit (16) is arranged so as to stop the operation after a predetermined execution time during execution of the algorithm and wherein the detection unit (18) is arranged so as to feed operational data into the algorithm at said predetermined execution time.

9. A device (10) according to one of the claims 1 to 3, wherein the algorithm is of such a nature that it will first randomize the input data (14), whereby the dependence of the operational data on the input data will be pseudo-random.

10. A device (10) according to claim 9, wherein the output data generated by the algorithm are only the operational data.

11. A device (10) according to one of the claims 1 to 4, wherein the electronic circuit (16) comprises two sub-circuits (16a, 16b) which each execute a sub-algorithm, the first sub-algorithm being a test algorithm whose operational data are detected by the detection unit (18), and the second sub-algorithm being a cryptoalgorithm or a check sum algorithm, the operational data of the test algorithm being processed in the cryptoalgorithm.

12. A device (10) according to claim 11, wherein the second sub-circuit (16a) is arranged so as to execute the DES algorithm which comprises n steps, and wherein the first sub-circuit (16b) is arranged so as to execute a test algorithm which also comprises n steps, the input data being adapted to be fed into the first step of the DES algorithm as well as into the first step of the test algorithm, and data which are adapted to be fed into a further step of the DES algorithm being result data of the first step of the DES algorithm and operational data of the first step of the test algorithm, whereas a result of one step of the test algorithm is rejected.

13. A device (10) according to one of the preceding claims, wherein the operational data detection unit comprises a time measuring means (18a) and a power measuring means

(18b) for measuring the time which the electronic circuit (16) needs for executing a specific task and for measuring the power consumed when said specific task is being executed.

14. A device (10) according to claim 13, wherein the power measuring means (18b) comprises a resistor, a capacitor and an analog-digital converter for measuring the power consumed.

15. A device (10) according to claim 13 or 14, wherein the time measuring means comprises an internal clock generator.

16. A device (10) according to one of the preceding claims, wherein the operational data detection unit (18) comprises a pattern recognition algorithm so as to produce the operational data from power or time parameters of the electronic circuit (16).

17. A method for checking the authenticity of a device to be tested in comparison with an examination device, the device to be tested and the examination device each comprising an electronic circuit (16) for executing an algorithm, which generates output data (12) on the basis of input data (14), and a unit (18) for detecting operational data which are influenced by an operation of the electronic circuit (16) and which depend on the input data, the operational data detection unit (18) of the device to be tested as well as of the examination device being coupled to the electronic circuit (16) in such a way that the operational data of the electronic circuit are used by the algorithm for producing the output data, said method comprising the following steps;

selecting (40) input data;

feeding (42) said input data into the device (10) to be tested;

in the device to be tested,

executing the algorithm by the electronic circuit of the device to be tested, so as to generate the output data on the basis of the input data,

detecting operational data of the electronic circuit, which are influenced by an operation of said electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by said electronic circuit (16), so as to generate the output data (12);

feeding (42) the input data into the examination device (10);

in the examination device

executing the algorithm by the electronic circuit of the examination device so as to generate the output data on the basis of the input data,

detecting operational data of the electronic circuit, which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by said electronic circuit (16), so as to generate the output data (12);

comparing (44) the output data of the device to be tested with the output data of the examination device; and

affirming (46) the authenticity of the device to be tested in comparison with the examination device if the output data correspond to one another, in such a way that authenticity will only be affirmed if the operational data of the device to be tested and of the examination device correspond to one another.

18. A method for encrypted transmission of information from a first to a second location, the second location being remote from the first location, comprising:

producing (50) a random word;

feeding (52) the random word into a first device implemented according to one of the claims 1 to 16 and arranged at the first location;

generating (54) the output data of the first device, which depend on the operational data of said first device, by executing an algorithm by the electronic circuit of said first device so as to generate the output data on the basis of the input data, operational data of the electronic circuit being detected, which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by the electronic circuit, so as to generate the output data;

encrypting (56) the information with the generated output data as a key;

transmitting (58) the encrypted information and the random word from said first location to said second location;

feeding (62) the random word into a second device implemented according to one of the claims 1 to 16 and positioned at the second location;

generating (64) the output data of the second device, which depend on the operational data of said second device, by executing the algorithm by the electronic circuit of said second device, so as to generate the output data on the basis of the input data, operational data of the electronic circuit being detected, which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by the electronic circuit, so as to generate the output data;

decrypting (66) the encrypted information making use of the output data of the second device as a key,

the decrypted information corresponding to the original information prior to encrypting if the operational data of the first device at the first location correspond to the operational data of the second device at the second location.